IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. KIRK COTTOM, Defendant.	8:13CR108 RESPONSE AND MOTION TO STRIKE DEFENDANT'S REQUEST FOR DAUBERT HEARING

COMES NOW the United States and hereby files this response to the defendant's motion for a *Daubert* hearing and moves to strike said motion. In support of this motion, the United States offers the following:

I. BACKGROUND

On April 9, 2015, the Court held a status hearing in this case to discuss various matters including whether the defendant was requesting a *Daubert* hearing regarding the government's use of a Network Investigative Technique ("NIT") to identify his true IP address. After hearing from the parties on that issue, the Court required that "[t]he defendant shall file a **Supported** Daubert Motion by the close of business on 6/26/2015." Dkt. 200 (emphasis added). The Court clearly articulated during the hearing that any such request would need to be supported by purported expert analysis regarding the reliability of the NIT. On June 25, 2015, the defendant filed a motion in limine/*Daubert* motion and memorandum in support that is unsupported by any purported expert testimony, reports, declarations or affidavits. Dkts. 215, 216. Instead, the defendant complains that he was not provided the "source code" to the government's Network Investigative Technique ("NIT"). The defendant makes no supported claims regarding the reliability of the NIT.

Also on June 25, 2015, the defendant separately provided two expert reports to the government, attached hereto as Exhibit 1. The defendant did not submit these reports to the Court in conjunction with his *Daubert* motion, nor did he cite to any portion of them in that motion. The reason is clear. As further described below, the defendant's experts unmistakably concluded that they successfully tested the NIT technology that identified the defendant's IP address and determined that it is "repeatable and reliable." Accordingly, because there is no contested issue as to the reliability of the NIT, there is no need for a *Daubert* hearing in this case.

The United States respectfully requests that the Court deny the defendant's request for a *Daubert* hearing. Based upon the parties' filings and the defendant's expert reports, there is no contested issue regarding the reliability of the NIT. Accordingly, the Court should find that the NIT is reliable and admissible at trial in this case and that its admission will not have an unfairly prejudicial effect that would outweigh its substantial probative value. Further, the United States requests that the Court vacate the scheduled July 27, 2015, date the Court had set aside for a potential *Daubert* hearing.

II. LEGAL STANDARDS

"Before admitting expert scientific testimony at trial, Rule 702 requires the district court to determine whether the testimony is based on a reliable scientific technique, and whether it will assist the jury." *United States v. Black Cloud*, 101 F.3d 1258, 1261 (8th Cir. 1996) (citing *United States v. Johnson*, 56 F.3d 947, 952 (8th Cir.1995)); *See also United States v. Kenyon*, 481 F.3d 1054, 1061 (8th Cir. 2007) (citing *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 589, 113 (1993) and *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141, (1999)). A non-exhaustive list of factors a trial court may consider in determining whether a technique is reliable includes: (1) whether the technique can be and has been tested; (2) whether the technique has been subjected to peer review and publication; (3) the known or potential rate of error for the technique and the existence and maintenance of standards for controlling the technique's operation; and (4) whether the technique is generally accepted in the scientific community. *Black Cloud*, 101 F.3d at 1261. As the Court stated in *Daubert*, the test of reliability is a “flexible” one, and *Daubert*'s list of specific factors neither necessarily nor solely applies to all experts or in every case. *Kumho Tire*, 526 U.S. at 141 (citing *Daubert*, 509 U.S. at 594). Even if expert scientific testimony is admissible under Rule 702, the district court may exclude the testimony if the testimony has an unfairly prejudicial effect that substantially outweighs its probative value. *Black Cloud*, 101 F.3d at 1261.

A district court enjoys “broad latitude when it decides how to determine reliability.” *Kumho Tire*, 526 U.S. at 142; see also *Kenyon*, 481 F.3d at 1061. “There is no requirement that the District Court always hold a *Daubert* hearing prior to qualifying an expert witness.” *Kenyon*, 481 F.3d at 1061 (citations omitted). “When a district court is satisfied with an expert's education, training, and experience, and the expert's testimony is reasonably based on that education, training, and experience, the court does not abuse its discretion by admitting the testimony without a preliminary hearing.” *Id.* (citations omitted); *but see United States v. Iron Cloud*, 171 F.3d 587, 590 (8th Cir. 1999) (finding abuse of discretion where trial court refused to hold a *Daubert* hearing to determine the reliability of a portable breath test (PBT) for blood alcohol level, which test was only a preliminary screening test whose results had been refused admission in numerous states, and where the court also failed to analyze whether admission of the test would be unfairly prejudicial).

III. ANALYSIS

The United States has provided notice of the NIT used to identify the defendant’s IP address in the instant case. Expert testimony about and evidence obtained from the NIT has previously been received by this Court in multiple trials. The NIT has been tested by defense experts and determined to be “repeatable and reliable.” Further, a search of the defendant’s computers revealed evidence of child pornography, use of the Tor network to obtain child pornography, and the unique Linux operating system and web browser identified by the NIT at the time it captured the defendant's IP address, further supporting the conclusion that the NIT functioned reliably in this case. Accordingly, there is no contested issue as to the reliability of the NIT. The Court should find the NIT to be a reliable scientific technique and that there is no danger of unfair prejudice that outweighs the NIT evidence's probative value.

a. The Government's Expert Notice

On November 7, 2014, the United States filed an expert notice pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure, disclosing that it intends to elicit testimony from Federal Bureau of Investigation ("FBI") Special Agent ("SA") Steven A. Smith, Jr. and FBI Supervisory Special Agent ("SSA") P. Michael Gordon, under Federal Rules of Evidence 702, 703, or 705. Dkt. 166, attached as Exhibit 2. Both SA Smith and SSA Gordon have testified as experts in multiple trials in the District of Nebraska. *See* United States v. Timothy DeFoggi, No. 13-CR-105; United States v. Joshua Welch, No. 13-CR-106; and United States v. Michael Huyck, No. 13-CR-107. Their respective CVs describing their qualifications are attached to the expert notice. In the trials of United States v. Joshua Welch and United States v. Michael Huyck, both SA Smith and SSA Gordon testified as experts regarding, *inter alia*, the use of the NIT to obtain identifying IP address information about the defendants in those cases. That evidence was received in those cases without objection and both defendants were convicted at trial.

The government's expert notice described in detail the function and operation of the NIT, which had previously been explained via numerous e-mails from the government to prior counsel for the defendant. In particular, the government's expert notice provided the following detailed description of the NIT technique:

You have previously been provided reports documenting data obtained via the use of the NIT, which includes IP address information, session identifier information, operating system and architecture type. We have also previously disclosed to you via e-mails dated September 4, 2014, and September 23, 2014,[1] incorporated herein by reference, details regarding where the particular NIT code was obtained and how it operated. In particular, as described in my September 4, 2014, e-mail message, the technique utilized a Flash application that, when downloaded by a user and activated by their browser, made a direct TCP connection to a server that the FBI controlled. Depending on the operating system and version of the user's browser, the connection would bypass the browser's configured proxy server and reveal the user's true IP address. In addition, the NIT also sent the user's operating system name and architecture type. Please also see my September 4, 2014 e-mail for example programming code for the Flash application itself. Further, as noted above and in my September 4 and 23 e-mails, the computer servers that hosted the pertinent websites contain the compiled code for the NIT. Those servers have been, and remain, available for examination by an expert of your choice. The experts disclosed herein may testify based upon their knowledge, skills, training and experience, as to any matters disclosed therein.

In order to avoid any confusion regarding the operation of the NIT, I offer the following further description of its functionality, about which the experts disclosed herein may testify. The NIT was a Flash application. Flash applications are commonly present on numerous Internet websites. The NIT did not consist of a virus or “malware.” The NIT took advantage of a potential vulnerability in the configuration of a user’s computer. When a user accessed a page on one of the pertinent websites where the NIT had been deployed, the NIT computer code would be downloaded to a user’s computer along with the images/text/content that made up that web page. If a user’s web browser was not configured to block Flash applications, then the NIT, once downloaded by a user’s computer, would cause the computer to send a communication (in other words, a request) to a government-controlled computer that revealed the computer’s IP address, a session identifier, the computer’s operating system and architecture. If a user’s web browser was configured to block Flash applications, then the NIT would not successfully cause the computer to send such a request. As of November of 2012, the up-to-date Tor browser bundle was configured to block such Flash applications. Accordingly, the NIT would not have revealed the IP address of such a user, or of a user who had manually configured his/her browser to connect to the Tor network and opted to block Flash applications. Because none of your clients were using the up-to-date Tor browser bundle to access the website in question, and none of your clients configured his computer to block Flash applications, the NIT successfully identified your client’s IP address.

[1] The date September 23, 2014, in the government’s expert notice was a typographical error. The correct date is October 23, 2014. The referenced e-mail messages are included as a part of Exhibit 2.

b. The Defendant's Experts Tested the NIT and Concluded that the NIT is "Repeatable and Reliable"

The defendant hired a team of experts, all of whom are professors at Dakota State University, to examine the NIT and its functionality.[2] The government made a copy of the website that the defendant is charged with accessing (TB2), including the compiled NIT code which was deployed therein, and copy of data from the computer server which collected information obtained via the NIT, available to the defendant's team of experts for analysis and review.

The defendant's team of experts conducted two separate analyses of the NIT technology.[3] After their analysis, the experts concluded that the NIT was "repeatable and reliable." Ex. 1 p. 27. The first analysis took place in January of 2015 and is recounted in Appendix A of the expert report. After that initial analysis, the experts reported the following:

> . . . the investigators can **<u>with certainty</u>**, **<u>confirm that the NIT can be tested and the process results in repeatable results</u>**. As the investigators confirmed these four pieces of information were in fact generated by the NIT. Furthermore, the investigators set up a test VM [Virtual Machine] to see if the information obtained by the NIT was repeatable and they had static results throughout their analysis. *Id.* p. 18 (emphasis added).

[2] According to their reports, the defendants' experts included: (1) Dr. Ashley Podhradsky, an Assistant Professor of Information Assurance and Forensics at Dakota State University. Ashley has a doctoral degree in Information Systems with a specialization in Computer Security from DSU. Ashley is also the program coordinator of the Masters of Science in Information Assurance and Computer Security program at DSU. In addition to her academic work, Ashley is the lead forensic examiner at a security consulting firm with presence in over 40 states. She has also given over 20 presentations at leading academic conferences such as Hawaii's International Conference on Systems Science and invited talks at top universities such as The Pennsylvania State University. Her Funded research is in the area of developing forensic procedures for non-traditional computing devices such as the Xbox gaming platform. She has been working on civil, criminal and private cases for 5 years; (2) Dr. Matt Miller, an Assistant Professor of Computer Science at Dakota State University and graduated from Kansas State University with a Ph.D. in Computer Science. At K-State Dr. Miller worked on modeling multiagent systems and parallel computing. He published to the both the International Journal of Computational Intelligence and the Journal Hydrology and Earth System Sciences. Dr. Miller has now switched focus on security and he teaches assembly programming, reverse engineering as well as graduate courses; and (3) Mr. Josh Stroschein, an instructor of Computer Science at Dakota State University. Josh is currently working on his doctorate in Cyber Operations at Dakota State. Josh has also worked as a Web Applications Developer for a private ecommerce site, and is a Senior Intelligence Operations Officer in the SD Air National Guard.

[3] According to the report from their initial investigation, the investigators were hired at the rate of $300 per hour with an estimated 75-100 hours of time needed to complete the case. Ex. 1 p. 28.

> . . . and through a testing on the investigators VM, **the investigators can confirm this process is both repeatable and reliable**. *Id*. p. 20 (emphasis added).
>
> The investigators found that the NIT was a fairly straightforward application. *Id*. p. 22.
>
> Given the NIT is using TCP, and TCP cannot be spoofed this provides further evidence of the NITs repeatability. *Id*. p. 23.
>
> A TCP connection is a very reliable way of transferring data and provides for ordered data transfer, retransmission, error correction and flow control. While there is no quantifiable data on the reliability of this method, TCP connections are the standard method of data transmission for critical over the internet based activity such as commerce, authentication, banking and the transmission of other sensitive data. *Id*. p. 27.

Ultimately, in a final summary of the initial report, the defendant's experts reported:

> The investigators believe that the NIT provided a **repeatable and reliable process of identifying true IP addresses**. *Id*. p. 27 (emphasis added).

In an e-mail message dated May 18, 2015, attached hereto as Exhibit 3, Dr. Podhradsky, the lead defense expert, recounted the results of the original analysis to FBI Special Agent Tarpinian:

> Hi Jeffrey,
> I wanted to touch base about our investigation outcome for the Cottom case. Long story short, **my team and I found that the NIT was repeatable** and Cottom had further questions he wanted flushed out as part of the investigation. Specifically they are attached. Mr. Cottom wasn't happy with our analysis however the judge wanted my team to continue on for this case . . . . Ex. 3 (emphasis added).

On account of the defendant's unhappiness with his expert team's initial conclusions, the defendant's experts conducted a second examination of the NIT in June of 2015. Their conclusion did not change. After that analysis, the experts reported the following further items and conclusions:

> . . . we were able to re-create the DNS server, the policy file server and the socket server. We successfully tested the configuration of Flash using Links2, Firefox and Rekonq[4] browsers. In the Rekonq browser logs were created by Cornhusker and

[4] "Rekonq" is a web browser for the Linux operating system. NIT and website data identified a Linux operating system and Rekonq browser was used to access TB2 when the NIT identified Cottom's IP address.

> the logs match the format given in the logs that were provided by the FBI. Ex. 1 p. 4.
>
> Mr. Cottem's [sic] IP address, sessionID's and the pages viewed match the FBI report. *Id*. p. 8.
>
> The correlation [between user activity and IP address identified by the NIT] was based on the SessionID, BoardID and the IP Address in the NIT logs. We do not believe that any errors exist for determining the IP Address, system information, BoardID and the SessionID. *Id*. p. 9.
>
> This data was sent to the client's browser and then the client's browser sent the data back to the socket server. We believe that the only manner, in which this could occur, was for a browser at the client's IP Address to request the page that contained the encrypted cookie. *Id*. p. 10.
>
> The investigators do not consider the NIT to be "hacking." The NIT exploited a configuration setting that did not require offensive-based actions. Exploitation is not always synonymous with hacking. In this situation the investigators believe that Flash worked as advertised. *Id*. p. 11.
>
> We were able to re-create the data that the NIT generated. *Id*. p. 13.
>
> The NIT worked with Rekonq. *Id*. p. 14.

c. Evidence Seized from the Defendant's Home Further Supports the Reliability of the NIT

On April 9, 2013, law enforcement agents executed a search warrant at the defendant's home in Rochester, NY. The defendant was interviewed and admitted using the Tor network. Located in the residence were two computers – a desktop and a laptop – that Cottom admitted he used. The desktop was a custom-built Linux-based computer on which the FBI found more than 3,000 suspected child pornography images and more than 4,000 references to Tor network websites, many which are known to FBI to be child pornography websites. Data extracted from numerous child pornography files on that computer revealed that they had been received from Tor network websites. Also found on that computer were 11 images which were available on the TB2 website as well as folders encrypted with the data encryption program eCfyptfs. The FBI also seized a Sony laptop computer from the defendant's home that was fully encrypted with TrueCrypt software. No examination has been able to be completed of that device due to the encryption.

As noted above, NIT and website data revealed that at the time the NIT identified the defendant's IP address accessing TB2, the user was using a Linux operating system and Rekonq browser. The seizure of a custom-built Linux computer from the defendant's home, on which there was a substantial amount of child pornography, substantial amount of evidence of access to Tor network websites including those known to contain child pornography, evidence that particular images of child pornography were in fact obtained via Tor network websites, and images that were available on the TB2 website, powerfully validates the NIT technology used in this case.

d. The Defendant's Request for the NIT "Source Code" is Moot

The defendant claims in his *Daubert* motion that he was not provided with the NIT "source code" which he asserts impacted his experts' evaluation of the NIT. His own expert reports contradict this allegation. Specifically, his experts concluded in no uncertain terms:

> The investigators requested the NITs source code in order to compare it to the decompiled Metasploit code from January however we did not receive it. While this could be interrupted [sic] as a setback, **the investigators do not believe it changes the outcome of their report. Meaning, through their analysis they were able to determine the functionality of the NIT regardless of having the NITs source code.** Ex. 1 pp. 3, 11 (emphasis added).

In addition to other materials, the government provided the defendant's experts with the "compiled" NIT code – i.e., the actual code as it existed on the TB2 website when the website operated and the defendant's IP address was identified. The defendant's experts were then able to "decompile" that code as necessary to further their analysis. Their ability to successful accomplish that task was thoroughly documented in their report, as follows:

> In performing their research, the investigators adhered to industry-accepted practices of analyzing source code and compiled applications. When source code is compiled, the result is a binary file that is an executable program. In the absence

> of source code, it is common practice to use decompilers to aid in the process of recovering source code from the program. In this case, those tools were already developed specifically for Flash applications and utilized by the investigators to recover source code from the compiled application. This process is more commonly referred to as reverse engineering. Ex. 1 p. 26.
>
> To acquire the source code, a decompiler is needed, and we used JPEX v.4.0.. Reverse engineering code is the standard method for extracting a program's functionality, given the fact that you don't have access to the source code . Reverse engineering is the time tested process to determine both functionality and acquire the original source code from binary files . The tool JPEX is a practioner [sic] and research tested application that has been used in the peer reviewed FPDective project to reverse engineer Flash applications and determine their functionality. Id. at 21-22.
>
> JPEX is a reputable tool that makes its source code freely available on Github , which allows for industry and research review. . . . De-compilation of the sample application by JPEX resulted in source code identical in functionality to that of the original application. There are minor variations in source code derived from dis-assembled code when compared to the original. The differences are not in functionality but in variable and function naming. The investigators found that the NIT was a fairly straightforward application. Id. at 22.

Accordingly, the defendant's experts were able to reach their conclusion that the NIT was "repeatable and reliable" using the compiled code provided for analysis. The defendant's request for the NIT "source code," which is unsupported by any declarations, affidavits, reports or other expert opinion, is therefore moot.

* * *

IV. CONCLUSION

There is no basis in law or fact for a *Daubert* hearing in this case. The government respectfully requests that the Court find based upon the parties' filings that the NIT is reliable and presents no danger of unfair prejudice that outweighs its probative value, and deny the defendant's motion for a *Daubert* hearing.

Respectfully submitted,

UNITED STATES OF AMERICA, Plaintiff

DEBORAH R. GILG
United States Attorney
District of Nebraska

By: s/ Michael P. Norris _
By: MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, Nebraska 68102
(402) 661-3700

s/Keith Becker _
KEITH BECKER
TRIAL ATTORNEY

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following: **Joseph L. Howard**, Attorney at Law, and also hereby certify that a copy of the same has been served by regular mail, postage prepaid, to the following non-CM/ECF participants:

s/ Keith A. Becker
Trial Attorney